Allscripts Enterprise

INFORMATION PRIVACY & SECURITY POLICIES: VENDOR SECURITY POLICY

Revision:	1.0
Approval Date:	February 11, 2019
Approval Authorities:	PSEC

For any comments or feedback related to this Policy, please email PandSCompliance@allscripts.com.

Summary of Changes

Date	Version	Summary of Changes	Author
04-Jan-19	1.0	Original	Maxwell

Approval Log

Date	Version	Approval Authority
11-Feb-19	1.0	PSEC

1.0 Contents

2.0 Purpose and Scope

- **"Vendor"** means a contractor, supplier, subcontractor, consultant, reseller, or agent, whether an individual or a company, that provides services or goods to or on behalf of Allscripts either directly to Allscripts or to another party on Allscripts behalf. A Vendor may be granted access to Allscripts Information Assets only if the following requirements are met:
    - there is a valid business purpose for the access,
    - there is a confidentiality agreement and/or privacy and security agreement, including, but not limited to a business associate agreement in addition to this document, in place, and
    - the Vendor returns or destroys Allscripts Information Assets at the end of the engagement or as soon as practical.
- Information is an asset that Vendors have a legal, regulatory, and contractual duty and responsibility to protect. Vendor's senior management is responsible for promoting the confidentiality, integrity and availability of Allscripts information in order to permit Allscripts to efficiently provide its products and services to clients.
- This Security Policy follows ISO 27002:2013[1] and provides a framework for the key policy directives and expectations of Vendors to support Allscripts business activities.
- Vendors shall develop and maintain an Information Security Management System to protect Allscripts assets, reputation, and Allscripts client data by building a culture that values privacy and security and by implementing effective security controls designed to protect the confidentiality, integrity, and availability of Allscripts Information Assets.

2.1 Continuous Improvement

- Vendor's Information Security Management System shall be built on the premise of continuous improvement and shall include the following
    - The evolving security threat landscape;
    - The changing business as Allscripts expands into new markets;
    - Vulnerabilities identified during risk management process;

[1] International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) International Standard ISO/IEC 27002:2013, *Information technology — Security techniques — Code of practice for information security management*

- Information from “best of breed” sources; and
- Data gained from continuously monitoring control effectiveness.

2.2 Applicability

- All members of the Vendor Workforce, including full and part-time employees, agents, independent contractors, and interns shall abide by this policy.
- Vendors with separate agreements, e.g., Business Associate Agreements, Master Services Agreements, shall also abide by the specific requirements in those agreements.
- Vendors shall ensure that their policies and procedures are inclusive of the requirements of this policy.
- Failure to comply with the requirements in this Policy may result in termination of Vendor’s contract with Allscripts or removal of individuals from working under Allscripts contracts and/or any other legal or equitable remedies available.

2.3 Lexicon

- For the purpose of this policy, the terms “**shall**,” “**should**,” and “**may**” are used with a specific policy requirement to denote the expectation of compliance.
  - “**Shall**” is an emphatic form of a requirement statement and is used to denote a mandatory action or condition. All policy statements containing the word “shall” implies that the actions shall be complied with and are not open to interpretation.
  - “**Should**” implies there is an accepted method, practice, or condition that is expected to be followed by all individuals. Exceptions may be made when conditions require alternative actions; however, ‘should’ does not grant the ability to ‘ignore’ or ‘disregard’ without appropriate justification and review.
  - “**May**” implies a statement of permitted action or support; however, there is no expectation of compliance.

3.0 Risk Assessment and Treatment

3.1 Assessing Security Risk

- Vendors shall perform regular privacy and security risk assessments as an integral aspect of their information security management system. The risk assessment shall identify, quantify, prioritize, and document risk:
  - **Identify:** Vendors shall assess what negative events, consequences or threats could occur if a vulnerability or

weakness is exploited. Risks shall be identified at an enterprise-wide (strategic) level, departmental (tactical) level and at an operational level (including technical vulnerability assessments).

- **Quantify**: Vendors shall follow a fact-based process to determine the *probability* and *impact* of each risk.
- **Prioritize**: Vendors shall prioritize quantified risks based on likelihood and impact on Allscripts operations, systems, data, or people. The Allscripts CSO shall evaluate the overall prioritization of risks to ensure they are in alignment with Allscripts business objectives. Vendors shall assign a risk owner for each risk that is responsible for addressing the risk to an acceptable level.
- **Document**: Vendors shall document the significant facts and the probability and impact if the event were to occur, including any corrective/mitigating action.

- Risk management is an on-going activity, not a one-time event. Vendors shall identify risks shall at the beginning of every major project or when a significant change occurs, and periodically reevaluated based on size, complexity, and scope.
- Vendors shall conduct Risk Assessments on a periodic basis, and at least annually.

3.2 Addressing Security Risks

- Once risks have been identified, quantified, prioritized, and documented, the Vendor shall develop an action plan using the steps below to address the risk. Allscripts may independently document and monitor key risks that impact Allscripts operations, systems, data, or people.
- Risks responses may include:
  - **Avoid** eliminate the risk altogether
  - **Transfer:** transfer the risk to a third party, e.g. insurance or indemnification through contractual language
  - **Accept:** accept any residual risk associated with the non-implementation of Security Policies, standards, or other security and control requirements
  - **Mitigate**: implement controls to diminish the probability or impact of a risk based upon a reasonable cost-benefit analysis

- Risk response measures shall include the evaluation of the tangible and intangible impacts of the risk against the tangible and intangible costs of the risk treatment.

- Vendors shall ensure that privacy & security risk remediation & mitigation activities are funded at an appropriate level.

4.0 Information Security Policies

- Vendors shall ensure that a set of policies for information security are defined, approved by Vendor's senior management, published, and communicated to Vendor employees, agents, independent contractors, and relevant external parties.

- Vendors shall be responsible for conducting reviews, at least annually, of their Security Policy and all related policies, standards, and procedures. Vendors shall also conduct an out-of-cycle review following the publication of any significant, new legal or regulatory requirements, and material changes to business practices that may affect the security of Allscripts Information Assets.

- Vendors shall maintain their security policies, procedures, and all previous versions for a minimum of six (6) years after the date it was last in effect, even if superseded.

5.0 Human Resources Security

5.1 Prior to Employment

- Vendors shall perform screening checks on all new members of their Workforce that will be in contact with Allscripts Information Assets, as appropriate and in accordance with relevant laws, regulations.

- Vendors shall develop a Code of Conduct and require all Vendor Workforce members to agree to, comply with, and sign the Code of Conduct on an annual basis.

5.2 During Employment

- Vendors shall ensure that privacy and security responsibilities are included in job descriptions and in terms and conditions of employment for Vendor Workforce members. Staffing and vendor contracts shall include similar provisions.

- Vendors shall develop annual privacy and security training for all Vendor Workforce members that includes compliance with the various laws and regulations that governs use & access to Allscripts Information Assets, such as HIPAA and/or GDPR. Vendors shall ensure that new hires complete the Privacy and Security training requirements within 30 days of joining the Vendor's Workforce.

- Vendors shall ensure that their Workforce with access to any Allscripts Information Assets are trained on their roles and responsibilities and have sufficient management oversight.

- Vendor shall maintain a master list of authorization rights granted to their members who have access to Allscripts Information Assets.

5.3 Termination or Change of Employment

- Upon termination of their employment, contract or agreement, all Vendor Workforce members shall return all equipments assets that store or process Allscripts Information Assets in their possession to the Vendor.

- Vendors shall ensure access rights are removed or modified for Allscripts Information Assets following termination or change of employment status of supervised staff.

6.0 Asset Management

6.1 Responsibility for Assets

- Vendors shall identify and maintain an inventory of equipment assets that store or process Allscripts Information Assets. Vendors shall be responsible for maintaining appropriate privacy & security controls, including access and availability. This includes tracking the location of all assets from on-boarding through disposal.

- PCs, laptops, tablets, smartphones and similar personally owned portable devices (aka, “BYOD”) shall not be used to access any Allscripts System, and/or Allscripts Information Assets without prior authorization from Allscripts IT Operations.

- Vendors shall secure access to equipment assets using multi-factor authentication (MFA) that meets NIST 800-63B Authenticator Assurance Level 2 (AAL2), as well as encryption that meets the current guidelines released by the US Department of Health and Human Services Office for Civil Rights for rendering unsecure protected health information unusable, unreadable, or indecipherable to unauthorized individuals.

6.2 Media Handling

- Vendors shall protect physical media including documents (both electronic and paper), computer media (e.g. tapes, disks, CD/DVD and USB drives, etc.), virtual storage (e.g., cloud-based storage), and system documentation from unauthorized access, use, disclosure, modification, removal and destruction.

- Vendors shall implement specific procedures for the collection, handling, and disposal of Allscripts Information Assets on removable and fixed media including the creation and storage of a Certificate of Destruction (CoD). These procedures shall ensure that data is destroyed at a level sufficient to meet applicable regulatory requirements, including NIST 800-88 Media Santization Guidelines.

6.3 Mobile Devices and Teleworking

- Vendors shall develop a telework security policy for Vendor employees who telework or work remotely. At no point shall a Vendor Workforce member store Allscripts Information Assets on a personally owned computing device (e.g., laptop, tablet, etc., commonly referred to as "bring your own device" (BYOD)), unless it has been approved in advance by Allscripts IT Operations.

7.0 Access Control

7.1 Business Requirement of Access Control

- Vendors shall establish and enforce formal documented access control procedures supporting this Policy regarding secure access to Allscripts Information Assets.

- Vendors shall implement appropriate technical safeguards to prohibit all access to information systems containing or processing Allscripts Information Assets unless specifically authorized through a formal process that validates the business need.

7.2 User Access Management

- Vendors shall implement access controls based upon the principles of Individual Accountability, Least Privilege, Minimum Necessary, and Separation of Duties. Access shall be granted or arrangements made for Vendor Workforce members according to their role, only to a level that shall allow them to carry out their duties.

- All users of Vendor information systems and all users that have access to Allscripts Information Assets shall have a unique credential (e.g., UserID & Password) and use multi-factor authentication (MFA).

- Vendors shall implement provisioning and de-provisioning processes for access to Allscripts Information Assets. Furthermore, Vendors shall implement procedures for adding or removing privileges within 24 hours of a change in role or employment status.

- Vendors shall review all accounts with access to Allscripts Information Assets at least twice annually, based on risk. Accounts that have been inactive for longer than 31 days shall be disabled.

7.3 System and Application Access Control

- Vendors shall employ unique user identification. Generic service accounts should not be used as a part of regular business operations. Use of default system accounts (e.g., administrator, root) shall be monitored and restricted to initial system setup.
- Vendors shall not enable Remote Desktop Protocol (RDP). RDP and other ther remote administration functions shall not be performed over the Internet.
- Vendor passwords shall follow recommendations outlined in NIST Special Publication 800-63-B. This includes, but is not limited to: password length & complexity requirements (for example, at least 10 characters containing mixed case, numbers, and special characters); throttling failed password attempts; and storing passwords salted using an appropriate hashing function such as PBKDF2.
- Vendor passwords shall be changed whenever there is any indication of possible system or password compromise, or within 24 hours after a user role change or termination. Default passwords shall be altered after installation of systems or software.
- Vendors shall verify user identities prior to password resets. When users are issued temporary passwords, they shall be required to change their password immediately at the first log-on. Temporary passwords shall be unique and non-guessable. Systems shall mask passwords that are being entered.
- Vendors shall set automatic screen lock or logoff after a predetermined period of inactivity (default of 15 minutes).
- Vendors shall maintain emergency access procedures for access to clinical information used for direct patient care.

8.0 Cryptographic Controls

8.1 Cryptographic Controls

- Vendors shall encrypt Allscripts Sensitive Information at-rest, in-motion, and (when possible) in-use.
- Data at-rest
    - Vendors shall take advantage of “always encrypt” options of their data storage solutions (e.g., MS SQL Server) to perform field- or column-level encryption where possible to secure Allscripts Sensitive Information while at-rest. Encrypted hardware solutions are not sufficient to meet the data at-rest encryption requirements.

  - Vendors shall inventory and document all locations where Allscripts Sensitive Information may be at-rest, including databases, message queues, log files, flat files, cloud storage, etc. Vendors shall provide this inventory to Allscripts upon request.

- Data in-motion
  - Vendors shall employ the latest versions of TLS (currently TLS 1.2) or message-level encryption to secure Allscripts Sensitive Information while in-motion.

- Data in-use
  - Vendors shall ensure that passwords, keys, and other similar information is encrypted in memory while in-use, where possible.

- In all cases, Vendors shall employ the latest ciphers and cryptographic technologies as recommended by NIST (i.e., FIPS 140-2 Annex A).
- Vendors shall develop a cryptograpic key management strategy that addresses secure key generation, key distribution, key storage, key rotation, and key revocation.
- Vendors shall provide Allscripts will evidence of such encryption.

9.0 Physical and Environmental Security

- Vendors shall ensure that facilities that create, receive, maintain, or transmit Allscripts Information Assets are protected by defined security perimeters, with appropriate security barriers and entry controls commensurate with identified risks. This includes provisions for gaining emergency access, if needed, to computing resources.
- Vendors shall ensure Allscripts Information Assets are physically protected from unauthorized access, damage, and interference.
- All members of the Vendor's workforce shall follow a clean desk policy with regards to Allscripts Information Assets. Vendors shall utilize screen savers and locking cabinets, including securing portable devices (e.g., laptops, thumb drives, etc.) when not in physical sight of workstations. Additionally, passwords shall never be written down on any physical media. Printers should be monitored to ensure hard copy printouts that may contain Allscripts Information Assets are not left unattended.

10.0 Operations Security

10.1 Operational Procedures and Responsibilities

- Vendors shall implement appropriate security policies and procedures to manage and operate all facilities used for processing Allscripts Information Assets in a secure manner following the Security Policy. Where appropriate, Vendors shall separate duties to reduce the risk of negligent or deliberate misuse of systems or information.

- Vendors shall implement electronic mechanisms to verify that Allscripts Information Assets have not been accessed, altered or destroyed in an unauthorized manner. These mechanisms shall include: security event log collection and retention; audit log & event log tampering detection; integrated log analysis and automated alerting; intrusion detection systems (IDS/IPS); and port filtering or server-level firewalls. Firewalls shall be installed to filter traffic between domains, block unauthorized access, and maintain separation of networks (e.g., separating the internal network from the DMZ). Vendor security staff shall review firewall configurations at least every six months. Any unaccounted for alerts that violate regular operational thresholds should be reported via the notification process outlined in the BAA or contract.

- Vendors who are developing systems shall include an audit capability for all access to Allscripts Information Assets to support regulatory requirements.

10.2 Protection from Malware

- Vendors shall take precautions to prevent and detect the introduction of malicious code and unauthorized mobile code.

- Vendors shall develop privacy & security training to address the risks of malware and shall require all users with access to Allscripts Information Assets to take this training at least once annually.

- Vendors shall ensure that anti-malware software is running on all systems, it cannot be disabled or bypassed by users, and that users are trained to monitor and report any suspicious activities or events. Vendors shall define a standard schedule for performing anti-malware scans. Where possible, “next generation” anti-malware technology shall be used that contiously monitors system files & processes.

- Vendors shall implement and maintian spam and anti-phishing solutions to identify, quarantine, and block suspected malicious traffic and/or payloads. Vendors shall occasionally test their workforce on their ability to identify spam and phishing attempts.

10.3 Back-up

- Vendors shall develop procedures to back-up and recover Allscripts Information Assets, and regularly test those procedures.
- Vendors shall ensure the escrow of code as contractually required.

10.4 Logging and Monitoring

- Vendors shall monitor access to computing assets containing Allscripts Information Assets to identify potential misuse, anomalies, unauthorized actions, and compliance. Vendors should implement a Security Operations Center (SOC) to support this monitoring.
- Unless longer retention periods are required by the Vendor's contract, Vendors shall retain security & audit logs as follows:
    - Application audit logs
        i. Description: Security logs (e.g., HIPAA audit trail) intended to be used by security & privacy officers for forensic reconstruction of security events.
        ii. Minimum Retention Period: 3 years
    - Medical records history & completeness logs
        i. Description: Clinical logs which show the sequences of actions (creates, updates, deletes, etc.) made to the legal medical record for a patient. Intended to be used by clinicians to reconstruct the sequence of clinical decisions or actions made to the patient's chart
        ii. Minimum Retention Period: 30 years; or as long as the legal medical record must be maintained
    - Infrastructure security logs
        i. Description: IIS logs, Windows logs, Syslogs, firewall logs, security tool logs, etc.
        ii. Minimum Retention Period: one year (Exception: audit logs related to the electronic prescription of controlled substances (EPCS) shall be retained for at least two years)
    - Error logs
        i. Description: Exception logs, developer logs
        ii. Minimum Retention Period: no required retention minimums

- Whenever a user performs a create, read, update, delete, copy, print, or query action on Allscripts Information Assets, the system shall create an audit log. The audit log shall include a unique user ID (or process identifier for automated events), a unique data subject ID, the function performed, the date/time that the event was performed, a pointer to the previous data state (for update and delete events), and a summary of the information affected by the action (e.g., type of patient information, filename, etc). Additionally, source and destination address should be captured for data transfer events. Audit tools should support report generation and user behavior monitoring. Auditing services shall meet high availability or guaranteed delivery standards.

- Vendors shall ensure that all relevant information processing systems (e.g., networks, servers, and workstations) are synchronized to a common external time source to assist with security investigations.

- Vendors shall peform vulnerability scans at least quarterly, or after any significant change in the network. Any issues identified shall be addressed as soon as reasonably possible, no longer than 30 days for critical issues and 60 days for high issues.**Control of Operational Software**

- Vendors shall secure system files from unauthorized access including program source code and operating system files.

- Vendors development and support teams shall implement procedures to ensure that all code changes are reviewed and approved prior to implementation into a production environment.

- Vendors shall implement procedures to blacklist unauthorized software or whitelist software.

10.6 Technical Vulnerability Management

- Vendors shall ensure controls are in place to perform effective, systematic, and repeatable technical vulnerability management of all environments that contain Allscripts Information Assets including the complete and timely identification of technical vulnerabilities, mitigation activities & controls, and monitoring the effectiveness of those controls.

- Vendors shall ensure the timely deployment of security patches, not longer than 30 days after critical or high severity security patches are released.

- Vendors who perform software development shall implement a Secure Development Lifecycle. All software shall follow a formal Software Development Life Cycle (SDLC) methodology as set forth in this Section and Section 12.1 below. No code may be placed into a

production environment prior to completing testing. No software shall be deployed that has known critical or high severity vulnerabilities.

- Vendors shall implement configuration management standards to address known security vulnerabilities and shall only enable services and protocols which are required for a business need.

10.7 Information Systems Audit Considerations

- Vendors shall maintain appropriate privacy & security certifications such as SSAE16 SOC2, HITRUST, or ISO.

- Vendors shall implement a continuous monitoring strategy including metrics to be monitored annually at a minimum, status tracking for non-compliant items, and implementing corrective action plans to address gaps. Third party audits (e.g., SOC2, ISO, or HITRUST) may be used to implement the continuous monitoring requirement.

11.0 Communications Security

11.1 Network Security Management

- Vendors shall develop procedures to appropriately manage and control networks from threats and to maintain security for the systems and applications which use the network.

- Vendors shall establish physically and logically separate networks. DMZs shall be used to protect internal networks; no Allscripts Information Assets shall be stored on servers in the DMZ.

- Vendors shall ensure that external traffic from the Internet shall pass through at least one load balancer, proxy server, firewall, or IDS/IPS which supports logging network sessions, source & destination checking, and whitelisting/blacklisting known bad actors.

- Vendors shall identify a list of users who have access specific networks and network services and specify the means of access allowed. Firewalls and other network-related restrictions shall be implemented to ensure users & processes only have access to systems & resources they have a business need to access. Remote access to Vendor networks containing Allscripts Information Assets shall be protected using multi-factor authentication and a VPN or similar secure connection. Unauthorized remote connections shall be monitored and disabled immediately upon detection.

11.2 Information Transfer

- Vendors shall use secured and encrypted communications channels to protect Allscripts Information Assets.

12.0 System Acquisition, Development and Maintenance

- Vendors involved with software development shall consider security requirements at all stages of the Secure Development Lifecycle (SDL) from conception and design through development and implementation and retirement of a production system as directed by Allscripts.
- The Vendor's SDL shall address security architecture reviews, threat modeling, security code reviews & scans, security testing, and secure configuration & deployment.
- Vendors shall not use Allscripts production data in development or test environments without approval by the Allscripts CSO.

13.0 Supplier relationships

13.1 Information Security in Supplier Relationships

- Vendors shall require their own vendors and subcontractors to follow the privacy & security requirements outlined in this policy, if those vendors or subcontractors are involved in accessing, processing, supporting, or maintaining Allscripts Information Assets.
- Vendors shall develop a process for monitoring their vendors and subcontractors for compliance.

14.0 Information Security Incident Management

- For the purposes of this Policy, all Privacy and Security Incidents shall follow the reporting procedures outlined in the BAA or contract.
- As appropriate, vendors shall maintain retainer agreements with cyber forensic and other cybersecurity specialists to assist in responding to privacy & security incidents.

15.0 Information Security Aspects of Business Continuity Management

15.1 Information Security Continuity

- Vendors shall implement and maintain a business continuity and disaster recovery (BC/DR) plan. Vendors conduct a Business Impact Analysis (BIA) which includes the consequences of disasters, security failures, loss of service, lack of service availability, and the probability and consequence of a significant interruption.
- Vendors shall determine appropriate Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO). Vendors shall regularly

review and test BC/DR plans to ensure they meet the target recovery objectives.

- Vendor's change management process shall include review of technical changes for their effect on BC/DR processes.

15.2 Redundancies

- Vendors shall implement disaster recovery and other technical controls using the principle of redundancy to ensure the complete restoration of all data identified as sensitive and critical.

- Vendors shall ensure that hosted Allscripts Information Assets are simultaneously stored in multiple geographically-separated data centers. Furthermore, critical services, such as DNS, shall have geographically separated redundant backups.

16.0 Definitions

- **Allscripts Information Asset** is a comprehensive term that includes Sensitive, Confidential, and/or Privileged Information, as those terms are defined in this policy.

- **Confidential Information** is all information, whether written or oral, about Allscripts, its clients, or its subcontractors that a reasonable recipient would consider confidential and/or proprietary, including but not limited to, trade secrets, source code, roadmaps, know-how, schema, algorithms, business plans, financials, client lists, inventions and patents documents. This information is only intended for internal distribution among Allscripts workforce members and authorized third parties (i.e., service providers and contractors/sub-contractors).

- **CSO** is the Chief Security Officer and is the individual designed in writing to act on behalf of Allscripts for all administrative, physical, and technical security issues as defined in 45 CFR §164.308(a)(2).

- **Privileged Information** is information that may be protected based on a legal relationship and may be protected from compelled disclosure in a court proceeding. Work product and communications developed under direction of, or for counsel, may be marked Privileged.

- **Sensitive Information** contains data elements that may be regulated, controlled, or otherwise designated as not public and therefore must be protected, such as Protected Health Information (PHI). "Sensitive Information" includes, but is not limited to, Protected Health Information (PHI), Personal Information (PI), Personal Health Information, Personal Data, employee data and Personally Identifiable Information (PII) (as those terms are defined in applicable law).

- **Workforce** means employees, contractors, third party users, volunteers, trainees, agents, and other persons whose conduct, in the performance of work for Allscripts, is under the direct control of Allscripts, whether or not they are on-site or off-site, and whether or not they are paid by Allscripts.